2018R000431/mfn/am

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
v.	:	Crim. No. 19- 770(SDW)
ANKUR AGARWAL	:	18 U.S.C. §§ 1030 and 1028A

INFORMATION

The defendant having waived in open court prosecution by indictment, the United States Attorney for the District of New Jersey charges:

Background

1. At all times relevant to this Information:

a. Ankur Agarwal ("Agarwal") resided in Montville, New Jersey.

b. Company One was headquartered in New York with offices in New Jersey and developed various technologies, including an emerging technology ("Emerging Technology"). Company One maintained and used computers and computer networks, and engaged in interstate business activities.

c. Company Two was headquartered in Texas with offices in New Jersey and developed various technologies, including the Emerging Technology. Company Two maintained and used computers and computer networks, and engaged in interstate business activities.

Hacking Scheme

2. From in or about February 2017 through in or about April 2018, Agarwal obtained unauthorized access to the computer networks of Company One and Company Two and stole data relating to the Emerging Technology.

Company One Intrusion

3. Beginning in or around February 2017, Agarwal physically trespassed onto Company One's premises in New Jersey and installed hardware key-logger devices onto Company One computers. The devices covertly recorded the keystrokes of Company One employees. Through the key-logger devices, Agarwal obtained numerous employees' login credentials. Agarwal also created and installed onto Company One's network a software program that acted as a digital key-logger. Through the digital key-logger, Agarwal obtained the login credentials of additional Company One employees.

4. While on Company One's premises, Agarwal installed and connected his laptop computer ("Personal Computer One") to Company One's computer network. Using the fraudulently obtained login credentials and Personal Computer One, Agarwal gained the ability to remotely access Company One's network without authorization.

5. After obtaining unauthorized remote access into Company One's network, Agarwal stole, transferred, and exfiltrated Company One's data.

6. Agarwal specifically targeted data related to the Emerging Technology and the employees assigned to work on the Emerging Technology ("Emerging Technology Team"). Beginning in or about March 2017, Agarwal created a computer code designed to exfiltrate data (the "Exfil Script"). From in or about March 2017 until in or about September 2017, Agarwal executed the Exfil Script

against multiple computers used by the Emerging Technology Team. Using these tactics and methods, Agarwal stole data relating to the Emerging Technology and personal information associated with multiple members of the Emerging Technology Team.

7. From in or about January 2018 to in or about February 2018, Agarwal targeted and obtained unauthorized access to the computers used by additional Company One employees, including its Chief Network Engineer Officer ("CNEO") and a network engineer.

8. In or about April 2018, Company One employees responsible for network security detected Agarwal's intrusion into the network and began an investigation. Agarwal, without authorization, accessed Company One's network and surveilled and eavesdropped on the investigation into his own activity.

Company Two Intrusion

9. In or about June 2016, Agarwal physically trespassed onto the premises of Company Two. Using the means of identification of another person, Agarwal fraudulently obtained an access badge that granted him continued access to Company Two premises in New Jersey. Agarwal installed onto Company Two's computers a hardware key-logger device that covertly recorded employees' keystrokes. Agarwal later recovered the key-logger device and fraudulently obtained several of Company Two's employees' login credentials.

10. While on Company Two's premises, Agarwal also installed and connected, without authorization, his laptop computer ("Personal Computer Two") to Company Two's computer network. By using fraudulently obtained employees' credentials and Personal Computer Two, Agarwal gained the ability to remotely access, without authorization, Company Two's computer network.

11. After gaining unauthorized remote access to Company Two's network, Agarwal stole, transferred, and exfiltrated Company Two's data and information. Among other things, Agarwal stole information about the Emerging Technology stored on Company Two servers. Beginning in or about April 2017, Agarwal used the Exfil Script to steal Company Two's email files and documents relating to the Emerging Technology, as well as personal documents relating to Company Two employees.

The Charges

Count One
(Obtaining Information from Protected Computers—Company One)

1. Paragraphs 1 through 11 of this Information are incorporated as though fully set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

ANKUR AGARWAL,

intentionally accessed a computer without authorization, and thereby obtained information from protected computers used in and affecting interstate commerce and communication, and the value of the information obtained exceeded $5,000:

Approximate Date	**Description**
February 2017	Agarwal accessed the computer assigned to Employee One and obtained information, including the login credentials of Employee One, instructional manuals relating to Company One's computer network, and approximately 700 additional files associated with Employee One.
February 2017	Agarwal accessed the computer assigned to Employee Two and obtained information, including the login credentials of Employee Two, Employee Two's security questions needed for account access, and a human resource file containing information about over 50 of Company One's senior management employees.
February 2017	Agarwal accessed the computers assigned to the End-User-Support ("EUS") Team and obtained information, including the login credentials of members of the EUS Team, manuals relating to Company One's computer systems, and over 7,000 email files associated with the EUS Team.
February 2017	Agarwal accessed the computer assigned to Employee Three and obtained information, including the login credentials of Employee Three, Employee Three's personal information, and over 8,000 email files associated with Employee Three.
March 2017	Agarwal accessed the computer assigned to Employee Four and obtained information, including email files and documents related to the Emerging Technology and Employee Four's personal information.
March 2017	Agarwal accessed the computer assigned to Employee Five and obtained information, including email files and documents related to the Emerging Technology.
March 2017	Agarwal accessed the computer assigned to Employee Six and obtained information, including email files and documents related to the Emerging Technology.
March 2017	Agarwal accessed the computer assigned to Employee Seven and obtained information, including email files and documents related to the Emerging Technology and Employee Seven's personal information.

Approximate Date	Description
September 2017	Agarwal accessed the computer assigned to Employee Eight and obtained information, including email files and documents related to the Emerging Technology and Employee Eight's personal information.
October 2017	Agarwal accessed the computer assigned to Employee Nine and obtained information, including email files and documents related to the Emerging Technology.
January 2018	Agarwal accessed the computer assigned to the CNEO and obtained information, including email files and documents related to the Emerging Technology.
February 2018	Agarwal accessed the computer assigned to the CNEO and obtained information, including email files and documents related to the Emerging Technology.

In violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(iii).

Count Two
(Obtaining Information from Protected Computers—Company Two)

1. Paragraphs 1 through 11 of this Information are incorporated as though fully set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

ANKUR AGARWAL,

intentionally accessed a computer without authorization, and thereby obtained information from protected computers used in and affecting interstate commerce and communication, and the value of the information obtained exceeded $5,000:

Approximate Date	Description
April 2017	Agarwal accessed Company Two's servers and thereafter obtained information and data related to the Emerging Technology.
April 2017	Agarwal accessed the computer assigned to Employee Ten and thereafter obtained email files and documents related to the Emerging Technology and Employee Ten's personal documents.

In violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(iii).

Count Three
(Aggravated Identity Theft)

1. Paragraphs 1 through 11 and Paragraph 2 of Count Two of this Information are incorporated as though fully set forth herein.

2. In or about May 2017, in the District of New Jersey and elsewhere, the defendant,

ANKUR AGARWAL,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, Title 18, United States Code, Section 1030(a) (computer fraud), knowing that the means of identification belonged to another actual person, namely, Agarwal transferred, possessed, and used the means of identification of an individual with the initials S.A., to obtain a Company Two access badge, and thereafter used the access badge

to maintain his unauthorized access to Company Two's premises in New Jersey for the purpose of furthering his hacking scheme.

In violation of Title 18, United States Code, Section 1028A(a)(1).

FORFEITURE ALLEGATION AS TO COUNTS ONE AND TWO

1. Upon conviction of the offenses in violation of 18 U.S.C. § 1030 alleged in Counts One and Two of this Information, Agarwal shall forfeit to the United States:

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts One and Two of this Information; and

b. pursuant to 18 U.S.C. § 1030(i), all right, title, and interest of the defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts One and Two of this Information, including, but not limited to: all right, title, and interest of the Defendant in the items listed in Attachment A hereto.

SUBSTITUTE ASSETS PROVISION

2. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

Craig Carpenito

CRAIG CARPENITO
United States Attorney

Attachment A

Item #	Make/Model/Description	Serial Number / Identifier
1	Western Digital My Book external hard drive	WX11DB5NE0HH
2	Western Digital My Book external hard drive (enclosure only)	N/A
3	Dark green rain jacket	N/A
4	Western Digital My Passport Ultra external hard drive with power cord	WXJ1AA5001VX
5	Dell Latitude E6430 laptop computer with power cord and cordless mouse	9CGMJX1
6	Black USB keylogger	N/A
7	Western Digital external hard drive	VLH3U53Y
8	Dell Latitude D630 laptop computer and power cord with Logitech wireless USB Bluetooth transmitter	DNWDDF1
9	Miscellaneous technical notes and Office Depot notepad	N/A
10	Nokia Microsoft RM1030 XL cellphone with power cord	740485700
11	Samsung Verizon 4G LTE cellphone	99000023037066
12	Acer Aspire 5742 laptop computer	LXR4F02002034465461601
13	iomega Screenplay SPMCAHD hard drive	83AJ32011X
14	Red National brand record notebook	N/A
15	3.5" Sony floppy disk	DEA B2405A
16	Staples 3 subject notebook	N/A
17	Five CD-R disks containing SafeGuard recovery and backup data	N/A
18	Power Spec external portable hard drive	V627361
19	Western Digital WD5000C032 external portable drive	WCAPW0003145
20	Toshiba 2 TB portable hard drive	14SATEGFT18B
21	Western Digital 2217Q external portable drive	VK0EL3XY
22	Dell E725 laptop computer	PKRNVWE725
23	EP Memory 1.0 GB SD card	N/A
24	Cruzer Mini 1.0 GB flash drive	N/A

Item #	Make/Model/Description	Serial Number / Identifier
25	Silver Dell GWZ8RW1 laptop computer with power cord	637230991978
26	Hewlett Packard 840G1 laptop computer (refurbished) with blue Ethernet cable	CNU409F0XD
27	USB keylogger	N/A
28	Black thumb drive with circle imprint	N/A
29	White CR203 2.0 thumb drive with "UBON" printed on it	N/A
30	Silver thumb drive with "Gemalto" and "Security to be Free" printed on it	N/A
31	Swipe card C-847930; AT&T tenant card in the name of Shashi Agarwal; AT&T contractor card in the name of Ankur Agarwal; Swipe card C0930024; Swipe card PP- 00878858	N/A
32	Samsung Galaxy S4 SGH-I337 cellphone with black Otter Box case	IMEI: 359721051256459
33	Samsung Galaxy Note 4 SM-N910V cellphone with Neo Hybrid black/silver case	IMEI: 990004812971194
34	Silver thumb drive	N/A
35	Black and red notebook with "Record" on spine	N/A
36	Two power adapters	N/A
37	Samsung Galaxy S4 SCH-I545UD cellphone with blue and black case	IMEI: 990004510333960

CASE NUMBER: 19-_____

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

ANKUR AGARWAL

INFORMATION FOR

18 U.S.C. § 1030
18 U.S.C. § 1028A

CRAIG CARPENITO
UNITED STATES ATTORNEY
NEWARK, NEW JERSEY

ANTHONY MOSCATO
MATTHEW FELDMAN NIKIC
ASSISTANT U.S. ATTORNEYS
973-645-2779